

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant :	Craig Lewis	Art Unit :	2137
Serial No. :	09/022,178	Examiner :	Minh T. Nguyen
Filed :	August 2, 2001	Conf. No. :	7529
Title :	SECURITY FOR STANDALONE SYSTEMS RUNNING DEDICATED APPLICATION		

Mail Stop Appeal Brief - Patents

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

BRIEF ON APPEAL

Appellant files this brief in conjunction with a Notice of Appeal after the final Office Action mailed August 28, 2006.

(1) Real Party in Interest

DRESSER, INC., the assignee of the present Application, is the real party in interest.

(2) Related Appeals and Interferences

There are no related appeals and interferences.

(3) Status of Claims

Claims 1-30 are pending in the application, with Claims 1, 13 and 24 being independent. Claims 1-7, 9-19, 21-27, 29 and 30 stand rejected. Claims 8, 20 and 28 are objected to.

(4) Status of Amendments

All amendments have been entered and no amendments are being submitted herewith.

(5) Summary of Claimed Subject Matter

A stand-alone computer system (*such as* 12, Page 3, Lines 15-21) having a password maintenance capability includes an operating system (*such as* 28, Page 3, Lines 26-27), a password generator (*such as* 42, Page 4, Lines 14-15), a password encryptor (*such as* 44, Page 4, Lines 14-15), and a display (*such as* Figure 5). The operating system (*such as* 28, Page 3, Lines 26-27) is operable for executing a dedicated application. The password security generator (*such as* 30, Page 4, Lines 14-15) couples with the operating system (*such as* 28, Page 3, Lines 26-27) for generating a password in response to an occurrence of a prescribed password generation event, in connection with the operating system (*such as* 28, Page 3, Lines 26-27) and the dedicated application. The password encryptor (*such as* 44, Page 4, Lines 14-15) couples to the password generator (*such as* 42, Page 4, Lines 14-15) for producing a coded password as a function of the generated password. The user can receive the generated password by provided the coded password to a remote password provider (*such as* Page 9, Lines 24-29).

(6) Grounds of Rejection

(A) Claims 1, 4-5, 9-10, 12-13, 16-17, 21, 23-26 and 29 are rejected for being non-obvious under 35 U.S.C. § 103(a) over U.S. Patent No. 6,601,175 to Arnold et al. ("*Arnold*") in view of U.S. Patent No. 6,718,468 to Challenger et al. ("*Challenger*"), and further in view of U.S. Patent No. 6,067,625 to Ryu ("*Ryu*").

(B) Claims 2-3 and 14-15 are rejected for being non-obvious under 35 U.S.C. § 103(a) over *Arnold* in view of *Challenger*, in view of *Ryu* and further in view of U.S. Patent No. 6,725,382 to Thompson et al. ("*Thompson*").

(C) Claims 6, 18 and 27 are rejected for being non-obvious under 35 U.S.C. § 103(a) over *Arnold*, in view of *Challenger*, in view of *Ryu*, and further in view of U.S. Publication No. 2004/0139349 of Henn et al. ("*Henn*").

(D) Claims 7 and 19 are rejected for being non-obvious under 35 U.S.C. § 103(a) over *Arnold*, in view of *Challener*, in view of *Ryu*, and further in view of U.S. Publication No. 2004/0031030 of Kidder et al. ("*Kidder*").

(E) Claims 11, 22 and 30 are rejected for being non-obvious under 35 U.S.C. § 103(a) over *Arnold*, in view of *Challener*, in view of *Ryu*, and further in view of U.S. Patent No. 5270943 to Warn ("*Warn*").

(7) Grouping of the Claims

- (A) Claims 2-12 rise and fall together with independent Claim 1;
- (B) Claims 14-23 rise and fall together with independent Claim 13; and
- (C) Claims 25-30 rise and fall together with independent Claim 24.

In so grouping the Claims, Appellant does not admit that the subject matter of dependent claims represents merely obvious variations under 35 U.S.C. § 103 over the subject matter of the respective independent claims.

(8) Argument

Generating a nonce fails to teach generating a password in response to an event

The combination of *Arnold*, *Challener*, and *Ryu* fail to teach each and every limitation of the claimed invention. For example, claim 1 recites, in part, "generating a password in response to an occurrence of a prescribed password generation event." Even though the Examiner offers the limited-use password disclosed in *Arnold* as the generated password, the Examiner attempts to argue that since the nonce, which is used to generate passwords, is generated each time the computer is turned on that, in effect, a limited-use password is generated each time the computer is turned on. In fact, *Arnold* explicitly teaches that the limited-use password is generated upon request, ***not a prescribed event***. In summary, the nonce is not a password and the limited-use password disclosed by *Arnold* is not generated in response to a prescribed event.

Arnold discloses generating a limited-use administrative password using a serial number, a control password, and a nonce. Col. 7, Lines 21-47. The enterprise administration obtains the serial number of a target computer system 16, the nonce generated by the target computer 16,

and a known control password. Col. 7, Lines 22-32. After obtaining these character strings, the enterprise administration then derives a machine-specific hash by concatenating the serial number and the control password and then hashing the resulting string using a non-reversible hashing algorithm. Col. 7, Lines 29-32; Col. 4, Lines 40-49. A limited-use hash is then computed by concatenating the machine specific hash and the nonce "and then hashing the input string with SHA-1 or some other *non-reversible* hashing algorithm." Col. 7, Lines 35-38 (emphasis added). The enterprise administration then converts the limited-use hash into a limited-use administrative password and provides this password to the user. Col. 7, Lines 41-47. Applicant submits that a new nonce may be generated each time the target computer 16 is turned but generating a new nonce does not mean that the limited-use password is generated each time the computer is turned on. In contrast, *Arnold* merely discloses that a limited-use password is generated "on an as-needed basis." *Arnold*, Col. 7, Lines 10-15. In other words, the offered password is generated *on request*, not in response to an occurrence of a prescribed password generation event.

Challenger teaches away from the proposed combination

For the sake of argument, even if generating the nonce is considered generating a password in response to a predetermined event, there is no suggestion or motivation to combine *Arnold*, *Challenger*, and *Ryu* for the teachings of the claimed invention. *Challenger* teaches away from using a remote third party to decode a coded password. In fact, *Challenger* teaches securing keys for decoding a package in either a secured memory or secured chip, *i.e.*, a remote party does not have access to the private key for decoding the encrypted package. Col. 2, Lines 9-22. In the previous Office Action dated August 28, 2006, the Examiner asserts that since *Challenger* teaches encrypting and decrypting messages that *Challenger* does not teach away from displaying a coded password for decoding by a remote party. However, "[a] prior art reference must be considered in its entirety, *i.e.*, as a whole, including portions that would lead away from the claimed invention." *W.L. Gore & Associates, Inc. v. Garlock, Inc.*, 721 F.2d 1540, 220 U.S.P.Q. 303 (Fed. Cir. 1983), cert. denied, 469 U.S. 851 (1984). (M.P.E.P. § 2141.02). Accordingly, Applicant submits that the Examiner has failed to consider *Challenger* in its entirety.

The Examiner speculates that "one of ordinary skill in the art would have been motivated ... so as to obtain the needed password for accessing the information." However, there is no

motivation to combine *Ryu's* password recovery system because *Challener* does not teach, suggest, or disclose the use of a decodable password such that a remote service center may decrypt the encrypted packaged. *Challener*, in contrast, teaches encrypting a first password and a random password into an encrypted package. The encrypted package is then stored locally in a hard disk. Col. 4, Lines 37-41. In the event that the encrypted packaged needs to be decrypted, the package is transferred to a secure device -- the signature chip 31. Col. 3, Lines 41-42. The public/private keys are retrieved from the protected storage area 33 and the signature chip 31 uses these keys to decrypt the package. Col.3, Lines 41-54. In short, *Challener* teaches away from a remote party decrypting the package because the keys for decrypting the package are either in the protected storage area 33 or the signature chip 31, a secure device. Applicant was unable to locate any passage that teaches that the private key may be provided to a remote party. In fact, the computer system disclosed in *Challener* is designed to prevent the disclosure, such as the display, of the encrypted package and, as a result, prevent remote systems or individuals from decrypting the package.

Independent Claims 13 and 24 recite limitations that are similar, although not identical, to the limitation of Claim 1 discussed above. Therefore, these claims are allowable for reasons analogous to those discussed above in connection with claim 1. Claims 16-17, 21, 23-26, and 29 each depend from one of independent claims 13 and 24 and are thus also patentable over the cited art.

The Office Action rejects claims 2-3 and 14-15 under 35 U.S.C. § 103(a) as being unpatentable over *Arnold* in view of *Challener* in view of *Ryu* and further in view of U.S. Patent No. 6,725,382 ("*Thompson*"). Also, the Office Action rejects claims 6, 18, and 27 under 35 U.S.C. § 103(a) as being unpatentable over *Arnold* in view of *Challener* in view of *Ryu* and further in view of U.S. Patent Publication No. 2004/0139349 ("*Henn*"). Further, the Office Action rejects claims 7 and 19 under 35 U.S.C. § 103(a) as being unpatentable over *Arnold* in view of *Challener* in view of *Ryu* and further in view of U.S. Patent Publication No. 2004/0031030 ("*Kidder*"). In addition, the Office Action rejects claims 11, 22, and 30 under 35 U.S.C. § 103(a) as being unpatentable over *Arnold* in view of *Challener* in view of *Ryu* and further in view of U.S. Patent No. 5,270,943 ("*Warn*"). Applicant traverses these rejections and all findings and assertions therein. In particular, these depend from one of independent claims 1,

13, and 24. As discussed above, independent claims 1, 13, and 24 are allowable over the combination of *Arnold*, *Challener*, and *Ryn*. The Office Action fails to cite any teaching or suggestion in *Thompson*, *Henn*, *Kidder* and *Warn* of the missing elements discussed above. Therefore, claims 2-3, 6, 7, 11, 14-15, 18, 19, 22, 27, and 30 are allowable at least because they depend from one of allowable claims 1, 13, and 24. Thus, Applicant respectfully requests that these rejections be withdrawn.

Allowable Subject Matter

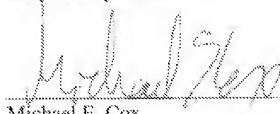
Applicant notes and appreciates the Examiner's indication that claims 8, 20, and 28 would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims. However, claims 8, 20, and 28 depend from one of Independent claims 1, 13, and 24, which Applicant respectfully submits are allowable. Accordingly, Applicant has not amended claims 8, 20, and 28 at this time.

The Commissioner is hereby authorized to charge the brief fee of \$500 to Deposit Account No. 06-1050. Please apply any other charges or credits to Deposit Account No. 06-1050.

Respectfully submitted,

Date:

Oct 30, 2006



Michael E. Cox
Reg. No. 47,505

Customer No.: **26231**
Fish & Richardson P.C.
1717 Main Street
Suite 5000
Dallas, Texas 75201
Telephone:
Facsimile: (214) 747-2091

Appendix of Claims

1. A method for maintaining a password in a computer system equipped with an operating system for running a dedicated application, comprising:

generating a password in response to an occurrence of a prescribed password generation event;

providing the generated password to an operating system security module;

producing a coded password as a function of the generated password, wherein the generated password can be determined by decoding the coded password;

displaying the coded password to a user of the computer system, wherein the user can receive the generated password by providing the coded password to a remote password provider; and

storing the coded password for use in connection with a secure operating system login access.

2. The method of claim 1, wherein providing the generated password to the operating system security module further includes overwriting a previously generated password.

3. The method of claim 1, wherein storing the coded password further includes overwriting a previously stored coded password.

4. The method of claim 1, further comprising:

displaying the stored coded password during an operating system login, wherein the displayed coded password is subject to being decoded with the use of a corresponding secure password provider, further wherein the secure operating system login is responsive to an input of a correctly decoded coded password for enabling access to the operating system as a function of the generated password and the operating system security module.

5. The method of claim 1, wherein the prescribed password generation event includes at least one selected from the group consisting of a computer system power-up; a computer system re-boot; expiration of a prescribed time duration from an immediately preceding password generation event; restoration of a security level from a modified security level to a default security level, and occurrence of a secure operating system login access.

6. The method of claim 5, wherein the modified security level of a password generation event includes at least one selected from the group consisting of a change in the security level within the dedicated application, a security level override within the dedicated application, and a one-shot security access within the dedicated application.

7. The method of claim 1, further comprising:
searching a username registry of the dedicated application upon the occurrence of the prescribed password generation event and removing any invalid usernames from the username registry.

8. The method of claim 7, further comprising:
reviewing privileges associated with respective valid usernames in the username registry and resetting the privileges of the respective valid username to prescribed default settings.

9. The method of claim 1, wherein generating the password includes generating the password for a prescribed username.

10. The method of claim 9, wherein the prescribed username includes a service username.

11. The method of claim 1, wherein the dedicated application includes a point of sale application in a fuel dispensing environment.

12. The method of claim 1, wherein the computer system includes at least one selected from the group consisting of a stand-alone computer system and a stand-alone network of computer systems.

13. A computer system having a password maintenance capability comprising:
an operating system including an operating system security module, an operating system data store module, and an operating system login module, said operating system operable for executing a dedicated application;

a password security generator including a password generator and a password encryptor, wherein

the password generator couples with said operating system for generating a password in response to an occurrence of a prescribed password generation event, the password generator providing the generated password to the operating system security module, and

the password encryptor couples to the password generator for producing a coded password as a function of the generated password, the password encryptor providing the coded password to the operating system data store module for use in connection with a secure operating system login access via the operating system login module, wherein the generated password can be determined by decoding the coded password; and

a display operable to display the coded password to a user of the computer system, wherein the user can receive the generated password by providing the coded password to a remote password provider.

14. The computer system of claim 13, wherein further the password generator provides the generated password to the operating system security module and overwrites a previously generated password.

15. The computer system of claim 13, wherein further the password encryptor stores the coded password and overwrites a previously stored coded password.

16. The computer system of claim 13, further comprising:

means for displaying the stored coded password during an operating system login, wherein the displayed coded password is subject to being decoded with the use of a corresponding secure password provider, further wherein the operating system login module is responsive to an input of a correctly decoded coded password for enabling access to said operating system as a function of the generated password and the operating system security module.

17. The computer system of claim 13, wherein the prescribed password generation event includes at least one selected from the group consisting of a computer system power-up; a computer system re-boot; expiration of a prescribed time duration from an immediately preceding password generation event; restoration of a security level from a modified security level to a default security level, and occurrence of a secure operating system login access.

18. The computer system of claim 17, wherein the modified security level of a password generation event includes at least one selected from the group consisting of a change in the security level within the dedicated application, a security level override within the dedicated application, and a one-shot security access within the dedicated application.

19. The computer system of claim 13, further wherein said password security generator further includes means responsive to an occurrence of a prescribed password generation event for searching a username registry of the dedicated application and removing any invalid usernames from the username registry.

20. The computer system of claim 19, further wherein the searching means reviews privileges associated with respective valid usernames in the username registry and resets the privileges of the respective valid username to prescribed default settings.

21. The computer system of claim 13, wherein the password generator generates the password for a service username.

22. The computer system of claim 13, wherein the dedicated application includes a point of sale application in a fuel dispensing environment.

23. The computer system of claim 13, wherein said computer system includes at least one selected from the group consisting of a stand-alone computer system and a stand-alone network of computer systems.

24. A computer program product for maintaining a password in a computer system equipped with an operating system for running a dedicated application, comprising:

a computer program processable by a computer system for causing the computer system to:

generate a password in response to an occurrence of a prescribed password generation event,

provide the generated password to an operating system security module,

produce a coded password as a function of the generated password, wherein the generated password can be determined by decoding the coded password,

display the coded password to a user of the computer system, wherein the user can receive the generated password by providing the coded password to a remote password provider, and

store the coded password for use in connection with a secure operating system login access; and

apparatus from which the computer program is accessible by the computer system.

25. The computer program product of claim 24, wherein said computer program is further processable by the computer system for causing the computer system to:

display the stored coded password during an operating system login, wherein the displayed coded password is subject to being decoded with the use of a corresponding secure password provider, further wherein the secure operating system login is responsive to an input of a correctly decoded coded password for enabling access to the operating system as a function of the generated password and the operating system security module.

26. The computer program product of claim 24, wherein the prescribed password generation event includes at least one selected from the group consisting of a computer system power-up; a computer system re-boot; expiration of a prescribed time duration from an immediately preceding password generation event; restoration of a security level from a modified security level to a default security level, and occurrence of a secure operating system login access.

27. The computer program product of claim 26, wherein the modified security level of a password generation event includes at least one selected from the group consisting of a change in the security level within the dedicated application, a security level override within the dedicated application, and a one-shot security access within the dedicated application.

28. The computer program product of claim 24, wherein said computer program is further processable by the computer system for causing the computer system to:

search a username registry of the dedicated application upon the occurrence of the prescribed password generation event and remove any invalid usernames from the username registry, and

review privileges associated with respective valid usernames in the username registry and reset the privileges of the respective valid usernames to prescribed default settings.

29. The computer program product of claim 24, wherein generating the password includes generating the password for a service username.

30. The computer program product of claim 24, wherein the dedicated application includes a point of sale application in a fuel dispensing environment.

Evidence Appendix

None

Applicant : Craig Lewis
Serial No. : 09/022,178
Filed : August 2, 2001
Page : 15 of 15

Attorney's Docket No. : 15828-160001 / PE-00-035

Related Proceedings Appendix

None